FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE SERGIPE - FANESE
NÚCLEO DE PÓS-GRADUAÇÃO E EXTENSÃO – NPGE
CURSO DE PÓS-GRADUAÇÃO "LATO SENSU"
ESPECIALIZAÇÃO MBA EM GESTÃO DE REDES E SEGURANÇA DA INFORMAÇÃO

GUILHERME DE SÁ TEIXEIRA

A SEGURANÇA EM TI NOS DIAS ATUAIS

IT SECURITY NOWADAYS

ARACAJU/SE
2016

GUILHERME DE SÁ TEIXEIRA

A SEGURANÇA EM TI NOS DIAS ATUAIS
IT SECURITY NOWADAYS

Artigo científico apresentado junto ao curso de MBA em Gestão De Redes e Segurança da Informação, como requisito à obtenção do título de profissional especialista em redes e segurança.

Orientação: Mestre Maria José de Azevedo Araújo

ARACAJU/SE

2016

SUMÁRIO

A SEGURANÇA EM TI NOS DIAS ATUAIS

IT SECURITY NOWADAYS

Guilherme de Sá Teixeira[1]

Orientação: Mestre Maria José de Azevedo Araújo[2]

RESUMO

Este trabalho apresenta o significado real da gestão em TI, e da segurança da informação, as maiores problemáticas enfrentadas por profissionais de TI, e os desafios enfrentados por esses profissionais no que diz respeito à segurança e alta disponibilidade dos dados da empresa no dia a dia. Serão também apresentadas as boas práticas de gestão, e algumas normas da segurança em TI.

Palavras-chave:

TI, Segurança, Dados, normas, profissionais, gestão

ABSTRACT

This paper presents the real meaning of management in IT and information security, the biggest problem faced by IT professionals, and the challenges faced by these professionals with regard to security and high availability of company data on a daily basis. good management practices will also be presented, and some security standards in IT.

Keywords:

IT, security, data, standards, professional, management

[1] Graduando MBA Em Gestão de Redes e Segurança da Informação pela Faculdade de Administração e Negócios de Sergipe.- FANESE. E-mail: guilherme.st@hotmail.com.

[2] Pedagoga, orientadora educacional, especialista em Educação, mestre em Educação e professora de cursos graduação e de pós-graduação de instituições de ensino superior do Estado de Sergipe. E-mail: professoraazevedo@gmail.com

1.0 - INTRODUÇÃO

> “O conhecimento passou a ser o principal fator de produção e geração de riquezas. “ (Bill Gates)

Diante do acelerado avanço tecnológico que está cada dia mais presente nas empresas, essas foram obrigadas com o passar dos anos a adequar-se, criando assim políticas e procedimentos de segurança importante para a segurança da informação, e consequentemente, gestão da empresa.

A segurança da informação está em constante evolução, assim como também as ameaças.

A segurança de informação não está ligada apenas à confidencialidade dos dados importantes da empresa como muitos pensam, o gestor de TI da empresa tem também o trabalho de assegurar alta disponibilidade, e segurança destas informações.

Todas as empresas buscam ter segurança e disponibilidade de dados no dia à dia, e isso torna a TI cada vez mais importante na gerência de negócios.

A leitura do presente artigo tem como objetivo esclarecer aos leitores o real significado da gestão, e da segurança em TI, a importância da boa gestão, serão também apresentados os perigos que a falta de segurança podem trazer aos usuários, os desafios enfrentados no dia a dia dos profissionais da área, serão também apresentadas algumas normas ABNT de segurança em TI utilizadas em todo o Brasil, e também boas práticas de gestão de TI, como o ITIL e o COBIT.

Também será explicado a necessidade de uma análise de risco prévia, para que haja implementação de segurança da melhor forma possível direcionada à necessidade da empresa.

2.0 - O QUE É SEGURANÇA DA INFORMAÇÃO?

A definição segundo a norma ABNT NBR ISO/IEC 27002 è a seguinte:

> A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectvidade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ver OECD Diretrizes para a Segurança de Sistemas de Informações e Redes).

A informação é uma das mais, senão a parte mais importante dos negócios de uma empresa e necessita estar sempre protegida, pois a informação è valiosa, e por ser, está cada vez mais visada como alvo para os hackers, e a diversidade e imensidão das ameaças é cada vez maior.

A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação è compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente. Porém, hoje em dia, a informação está presente predominantemente no meio digital,e a tendência é ela estar cada vez mais, daí então a importância da segurança em TI

A Segurança da informação em uma corporação é no geral, a àrdua tarefa que cabe à gestão da TI da organização de proteger da informação em seus variados tipos, de qualquer tipo de ameaças para garantir a continuidade do negócio, minimizar prejuízos.

A segurança da informação só pode ser obtida através da implementação de um conjunto de políticas, controles, processos… Esses controles precisam ser previamente analisados, realizando análises de risco, para então serem implementados, e constantemente adequados para garantir a segurança da organização. ”Convém que isto seja feito em conjunto com outros processos de

gestão do negócio., ABNT NBR 27002.”

Para a norma ABNT NBR ISO/IEC 17799, que mais tarde teria sua numeração atualizada para 27002, as 3 fontes principais de de segurança da informação são elas:

- Análise de risco da empresa, por meio dessa análise são identificadas as ameaças e as vulnerabilidades que a empresa em questão está sujeita.
- A legislação vigente , a regulamentação e as cláusulas entre a empresa e seus parceiros , funcionários tem que atender
- Um conjunto de princípios, objetivos e requisitos do negócio para processar a informação

3.0 - PRINCIPAIS DESAFIOS À GESTÃO DA SEGURANÇA EM TI

Para Jason Porter, os malwares destrutivos estão se espalhando com mais rapidez e abrangencia.

Enquanto o crimeware – como os keyloggers ou os trojans que roubam senhas – têm sido tipicamente o malware mais comum dos quais as empresas precisam se proteger, novos tipos destrutivos de malwares estão agora surgindo. Ataques no estilo do Wiper e dos trojans ransomware estão sendo postos à solta por ciberterroristas e grupos criminosos.

Os hackers/ativistas também estão adotando essas novas armas à medida que as organizações ganham a habilidade de mitigar as consequências dos ataques distribuídos de negação de serviço. Além disso, malwares destrutivos estão agora sendo disseminados para os ambientes mobile.

Preparar-se para esses tipos de ataques é uma tarefa crucial. As empresas estão utilizando a segurança e a análise de rede para melhorar a detecção de atividades mal-intencionadas antes que elas se consolidem e para se recuperarem mais rapidamente de incidentes com backups off-line.

A nova moda da atualidade se chama Ransonware, são softwares mal-intencionados (malwares), onde o hacker que instala de algum local no seu computador, e assim o “sequestra”, segundo a Microsoft, a definição de Ransonware é: “Ransomware é uma espécie de malware (software mal-intencionado) que os criminosos instalam em seu computador sem seu consentimento. O ransomware dá

aos criminosos a possibilidade de bloquear seu computador de um local remoto. Depois, ele apresenta uma janela pop-up com um aviso de que seu computador está bloqueado e você não poderá acessá-lo, a menos que pague.” A instalação do ransonware se dá pelos mesmos meios dos outros vírus, por email com anexo infectado, sites mal intencionados, arquivos de fontes duvidosas, por exemplo.

Outro grande problema da atualidade são a adoção do BYOD, ou bring your own device, que tem aumentado e muito os riscos de infecção, pois hoje em dia existem muitos vírus que infectam pen drives, espalhando assim o malware conforme ele é plugado em outros computadores.

Traze-los para o ambiente corporativo apresenta muito risco para a segurança, mas para isso existem softwares que podem ser usados para bloquear a entrada USB do computador. Mas, o maior desafio enfrentado por gestores de TI, desde sempre são os usuários dos computadores da empresa. Estes são os maiores inimigos, não que seja a intenção deles prejudicar, mas, por falta de conhecimento na área, acabam clicando em links não confiáveis, abrindo e-mails infectados, trazendo dispositivos próprios infectados, sejam eles pen drives, celulares, notebooks. Na maioria das empresas a preocupação com problemas maiores é muito focada, e problemas menores e menos visíveis acabam sendo esquecidos.

Deve-se também ficar atento para problemas não só dos dias de hoje, problemáticas essas que sempre deverão ser observadas de perto, como por exemplo, ter uma rotina de Backup bem definida para evitar perdas de dados, garantindo que nenhum arquivo de importância seja perdido, disponibilidade dos Ativos importantes de TI, colocando-os em nobreaks de forma que garanta que os mesmos nunca sejam desligados sem planejamento prévio, atentar e conscientizar funcionários para a problemática da engenharia social, que é muito usada pelos hackers para obtenção de dados cruciais da empresa, como senhas, ou outros dados.

4.0- MEIOS DE SE PROTEGER

Hoje em dia, com o crescente perigo dos perigos enfrentados pelas organizações, os softwares e sistemas que servem para nos blindar também evoluem. Hoje em dia os softwares anti vírus mais utilizados nas empresas são o Mcafee e o Kaspersky. Com estes temos como gerenciar os dispositivos que poderão ser conectados ao

computador, bloqueando assim uso de pen drives por exemplo, impedindo assim um dos maiores problemas da atualidade, o BYOD.

Os dois softwares possuem também um módulo firewall que cria uma barreira de proteção computador, gerando relatórios de tentativas de invasão. Pode-se também ser gerado um relatório de acesso à sites por estação no qual podemos identificar quem acessou sites indevidos, botando em risco a empresa.

Estes softwares de gerência são os melhores amigos dos gestores de segurança.

Podemos também fazer uso de firewalls e proxys para melhor proteção e monitoramento, como por exemplo o Pfsense e o squid, que funcionam em plataforma linux.

Um estudo feito pela McAfee, uma das maiores empresas do mundo em soluções de segurança na web, previu que 2015 finalizaria como o ano com maior número de ataques cibernéticos via internet, especialmente por conta da grande demanda de conexões móveis (smartphones e outros objetos conectados). Daí a importância de relembrarmos a importância de um firewall para a sua empresa.

5.0 - NORMAS DE SEGURANÇA DA INFORMAÇÃO:

5.1 NBR 17799

A norma ISO/IEC 17799 foi criada no ano 2000 no Brasil, que era uma cópia fiel à norma britânica BS 7799-1:1999, e que por fim em setembro de 2001 a ABNT homologou a versão brasileira denominada NBR ISO/IEC 17799, e que mais tarde seria atualizada para a numeração ABNT ISO/IEC 27002 em julho de 2007. Era composta por 11 seções.

5.2 ABNT NBR ISO/IEC 27002

A norma ABNT ISO/IEC 27002, também conhecida como o código de prática para Gestão de Segurança da informação, ela tem o objetivo de melhorar a gestão de segurança, trata-se de um manual de boas práticas de segurança em TI na qual é descrita desde a avaliação de riscos, como lidar nas mais diversas situações de incidentes que possam ocorrer, até a avaliação de riscos do meio físico da

informação. Se encontra dividida em 15 seções, as principais começam na quarta, são elas:

04 - Análise/Avaliação e tratamento de riscos
05 - Política de segurança da informação
06 - Organizando a segurança da informação
07 - Gestão de Ativos
08 - Segurança em Recursos humanos
09 - Segurança física e do ambiente
10 - Gerenciamento das operações e comunicações
11 - Controle de acesso
12 - Aquisição, Desenvolvimento e manutenção de sistemas de informação
13 - Gestão de incidentes de segurança da informação
14 - Gestão da continuidade do negócio
15 - Conformidade.

5.3 Norma ABNT NBR ISO/IEC 27001

Esta norma foi publicada em 10/2005 e substituiu a norma BS 7799-2 para certificação de sistema de gestão de segurança da informação. Norma essa Elaborada para prover um modelo para implementar, operar, monitorar, analisar criticamente, manter e melhorar um sistema de gestão de segurança da informação.
Nas duas normas 27001 e consequentemente 27002, a gestão de continuidade é citada como fator crítico de sucesso para a proteção da informação, e a gestão de continuidade é melhor explicada no Itil.

6.0 ITIL

Com o avanço da tecnologia, as organizações se tornam cada vez mais dependentes da Tecnologia da informação, então são cada vez também mais relacionados como base para o crescimento dessas empresas. Boas práticas de gestão se tornam indispensáveis para que seja oferecido o menor risco possível, proporcionando segurança dos dados em conformidade com todas as leis, para que

haja também redução de custos, tornando assim a TI uma parceira estratégica. Para alcançar essa integração TI-empresa, a adoção das práticas listadas na Information technology infrastructure library tem sido um caminho cada vez mais adotado.

O ITIL é um conjunto de boas práticas de gestão à serem aplicadas na infraestrutura para o melhor gerenciamento de serviços de TI. “Sua primeira versão foi desenvolvida em 1980 pela CCTA(Central computer and telecommunications agency), hoje OGC (office for government commerce) do Reino unido”(wikipedia).

A versão inicial do ITIL consistia em uma biblioteca de 31 volumes, cobrindo todos os aspectos do Gerenciamento de Serviços de TI (GSTI). Em meados de 1990, o ITIL foi reconhecido como um "padrão de fato", no Gerenciamento de Serviços de TI (GSTI) ou *IT Service Management* (ITSM). Posteriormente a versão inicial foi revisada e substituída pela **ITIL v2** (versão 2), que consistia em 7 volumes. O **ITIL v2** se tornou a base padrão para a norma BS 15000, que se tornou um anexo da norma ISO 20000.

Em maio de 2007, foi lançada ITIL v3 (também conhecida como *ITIL Refresh Project*) consistindo de vinte e seis processos e funções, agora agrupadas sobre somente cinco volumes, arranjados sobre conceitos sobre uma estrutura de ciclo de vida de serviços.

Em 2009, o OGC anunciou oficialmente que ITIL v2 poderia ser descontinuado e lançou uma consulta de como poderia proceder.

6.1 Segurança da informação e o ITIL

A utilização do Itil é de suma importância na segurança em TI, por conta de alguns assuntos importantes citados na biblioteca, como por exemplo: gerenciamento da disponibilidade, trata deste que é um dos maiores requisitos da segurança da informação, explicando como é feito um plano de disponibilidade, garantindo que a disponibilidade adequada seja entregue à serviços de TI, auxiliando também na identificação de funções vitais do negócio , vale ressaltar que gestão de disponibilidade trata apenas de requisitos de segurança, que são atributos que devem ser levantados na fase de planejamento. Com um pouco de intimidade na segurança em TI é possível perceber a importância da gerencia de continuidade, continuidade e segurança são temas relacionados, quando se trata de segurança.

Todos esses tópicos acima citados são de grande importância o entendimento e aplicação para maior segurança na TI. Porém o tópico do Itil mais importante se chama “Gerenciamento da segurança da informação para TI”, pois contempla o processo da segurança como um todo, resumindo as boas práticas para a gestão da segurança da informação.

7.0 COBIT

“COBIT®, do inglês, *Control Objectives for Information and related Technology*, é um guia de boas práticas apresentado como *framework*, sendo dividido em 4 domínios que possuem 34 processos com 318 objetivos de controle, abrangendo amplamente a operação de TI. Ele possui uma série de recursos que podem servir como um modelo de referência para gestão da TI, incluindo um sumário executivo, um *framework*, objetivos de controle, mapas de auditoria, ferramentas para a sua implementação e principalmente, um guia com técnicas de gerenciamento.[1] Especialistas em gestão e institutos independentes recomendam o uso do Cobit como meio para otimizar os investimentos de TI, melhorando o retorno sobre o investimento (ROI) percebido, fornecendo métricas para avaliação dos resultados (Key Performance Indicators KPI, Key Goal Indicators KGI e Critical Success Factors CSF).

O Cobit independe das plataformas adotadas nas empresas, tal como independe do tipo de negócio e do valor e participação que a tecnologia da informação tem na cadeia produtiva da empresa.

Em dezembro de 2007, foi lançado o COBIT 4.1, com maiores implementações em relação à versão anterior, 3.0, lançada em 2003.

“O COBIT 5 é a atual versão do *framework*. Uma das principais alterações em relação ao COBIT 4.1 é a integração com outros conjuntos de boas práticas e metodologias, como padrões ISO, ITIL, dentre outros. ” (Wikipedia).

Durante a última década, o termo ‘governança’ ganhou um lugar de destaque no pensamento das organizações em resposta aos exemplos que demonstram a importância da boa governança e, do outro lado da balança, aos desafios dos

negócios globais.Organizações bem-sucedidas reconhecem que a diretoria e os executivos devem aceitar que a TI é tão significativa para os negócios como qualquer outra parte da organização. Diretores e gestores - seja em funções de TI ou de negócios - devem colaborar e trabalhar em conjunto a fim de garantir que a TI esteja inclusa na abordagem de governança e gestão. Além disso, cada vez mais leis e regulamentos estão sendo aprovados e estabelecidos para atender a essa necessidade.

O COBIT 5 fornece um modelo abrangente que auxilia as organizações a atingirem seus objetivos de governança e gestão de TI. Em termos simples, O COBIT 5 ajuda as organizações a criar valor por meio da TI mantendo o equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e de utilização dos recursos. O COBIT 5 permite que a TI seja governada e gerida de forma holística para toda a organização, abrangendo o negócio de ponta a ponta bem como todas as áreas responsáveis pelas funções de TI, levando em consideração os interesses internos e externos relacionados com TI. O COBIT 5 é genérico e útil para organizações de todos os portes, sejam comerciais, sem fins lucrativos ou públicas.

O Cobit 5 se baseia em 5 princípios básicos, são eles:

7.1 - 1º Princípio:

Atender às Necessidades das Partes Interessadas - Organizações existem para criar valor para suas Partes interessadas mantendo o equilíbrio entre a realização de benefícios e a otimização do risco e uso dos recursos. O COBIT 5 fornece todos os processos necessários e demais habilitadores para apoiar a criação de valor para a organização com o uso de TI. Como cada organização tem objetivos diferentes, o COBIT 5 pode ser personalizado de forma a adequá-lo ao seu próprio contexto por meio da cascata de objetivos, ou seja, traduzindo os objetivos corporativos em alto nível em objetivos de TI específicos e gerenciáveis, mapeando-os em práticas e processos específicos.

7.2 – 2º Princípio:

Cobrir a Organização de Ponta a Ponta - O COBIT 5 integra a governança corporativa de TI organização à governança corporativa:

– Cobre todas as funções e processos corporativos; O COBIT 5 não se concentra somente na 'função de TI', mas considera a tecnologia da informação e tecnologias relacionadas como ativos que devem ser tratados como qualquer outro ativo por todos na organização.

– Considera todos os habilitadores de governança e gestão de TI aplicáveis em toda a organização, de ponta a ponta, ou seja, incluindo tudo e todos - interna e externamente - que forem considerados relevantes para a governança e gestão das informações e de TI da organização.

7.3 – 3º Principio:

Aplicar um Modelo Único Integrado - Há muitas normas e boas práticas relacionadas a TI, cada qual provê orientações para um conjunto específico de atividades de TI. O COBIT 5 se alinha a outros padrões e modelos importantes em um alto nível e, portanto, pode servir como o um modelo unificado para a governança e gestão de TI da organização.

7.4 – 4º Principio:

Permitir uma Abordagem Holística - Governança e gestão eficiente e eficaz de TI da organização requer uma abordagem holística, levando em conta seus diversos componentes interligados. O COBIT 5 define um conjunto de habilitadores para apoiar a implementação de um sistema abrangente de gestão e governança de TI da organização. Habilitadores são geralmente definidos como qualquer coisa que possa ajudar a atingir os objetivos corporativos. O modelo do COBIT 5 define sete categorias de habilitadores:

1. Princípios, Políticas e Modelos
2. Processos
3. Estruturas Organizacionais

4. Cultura, Ética e Comportamento
5. Informação
6. Serviços, Infraestrutura e Aplicativos
7. Pessoas, Habilidades e Competências.

7.5 – 5º Princípio:

Distinguir a Governança da Gestão – O modelo do COBIT 5 faz uma clara distinção entre governança e gestão. Essas duas disciplinas compreendem diferentes tipos de atividades, exigem modelos organizacionais diferenciadas e servem a propósitos diferentes. A visão do COBIT 5 sobre esta importante distinção entre governança e gestão é:

7.5.1 Governança

Na maioria das organizações, a governança geral é de responsabilidade do conselho de administração sob a liderança do presidente. Responsabilidades de governanças especificas podem ser delegadas a modelos organizacionais especiais no nível adequado, especialmente em organizações complexas de grande porte.

7.5.2 Gestão

Na maioria das organizações, a gestão é de responsabilidade da diretoria executiva sob a liderança do diretor executivo (CEO). Juntos, esses cinco princípios permitem que a organização crie um modelo eficiente de governança e gestão otimizando os investimentos em tecnologia da informação e seu uso para o benefício das partes interessadas.

8.0 Segurança da informação e o Cobit

O guia Cobit 5 for information Security , parte da família de publicações do cobit 5, que foi lançado em meados de 2012 como dito acima, está dividido em 3 seções principais, são elas:

1- Segurança da informação
2- Usando os facilitadores na implementação de segurança da informação na prática

3- Adaptando o Cobit 5 no ambiente corporativo

Para Christos Dimitriadis, Vice presidente da ISACA, o guia COBIT 5 pode ajudar as empresas na redução de seu perfil de riscos quando a segurança é gerenciada de forma correta. É claro que a informação e toda a tecnologia associada à ela tem se tornado cada vez mais o centro de atenções das empresas, mas a segurança tem sido deixada de lado. Sendo assim, aplicando-se o uso correto de boas práticas, como o exemplo do COBIT, que é composto de princípios mundialmente aceitos, bem como de ferramentas e modelos de análises desenvolvidos para suportar o negócio e a TI, podemos obter o melhor resultado possível, maximizando o grau de confiança e o valor que o mercado deposita nas operações da empresa.

9.0 - A importância da análise de risco

A análise de risco é importante pois assim podemos identificar os ativos de prioridade crítica, e que necessitam de mais atenção, para que então possamos elaborar um melhor plano de segurança em cima dessa análise, garantindo assim uma alta disponibilidade desses ativos, e também planejando uma norma e política de segurança mais direcionada à TI da empresa em questão, pois cada empresa tem a sua particularidade.

Em artigo publicado no iPlanner, Armin Laidre, co-fundador da plataforma de gestão de mesmo nome, explica que identificar e discutir esses riscos ajuda a fortalecer o plano, além de aumentar a credibilidade da administração e aumentar a confiança de potenciais investidores.

Para Laidre, a análise de risco é especialmente importante para startups e empresas menores, que estão iniciando sua trajetória no mundo dos negócios. De acordo com ele, empresários responsáveis por essas empresas ainda não conseguem identificar os riscos que podem vir a prejudicar seus negócios no futuro.

CONSIDERAÇÕES FINAIS

Conclui-se que, com a utilização dos métodos e seguindo as normas da boa segurança, é possível minimizar ao máximo os estragos e perigos que são passados no dia à dia.

Com a leitura do presente artigo, é esperado que a compreensão do leitor tenha sido clara em relação à importância da segurança em TI no meio empresarial.

Meios de se prevenir e proteger foram apresentados, como foi dado o exemplo dos softwares ante vírus , proxys, e firewalls, e o uso deles foi explicado, para melhor entendimento de qual seria sua utilidade na empresa.

Também, a problemática do usuário que sempre está, e sempre estará presente. Foi mostrado também o novo mal que tem atacado muitos usuários pelo mundo, os ransonwares, e também a importância do uso do ITIL e COBIT na gerencia da segurança da informação das empresas, que são essenciais para o sucesso do negócio.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Cobit 5:** Um modelo corporativo para a governança e gestão de TI da organização. http://www.pmgacademy.com/images/pdf/cobit5-pt.pdf

CESTARI FILHO. **f. ITIL V3 Fundamentos.** Rio de Janeiro: Escola Superior de Redes, RNP, 2011

FONTES, Edison. **Segurança da Informação:** O usuário faz a diferença, Editora Saraiva, 2005.

http://computerworld.com.br/Novos-desafios-para-seguranca-no-segmento-de-ti

http://destinonegocio.com/br/Financas/saiba-a-importancia-da-analise-de-risco-nos-negocios/

http://www.abntcatalogo.com.br/Norma.aspx?ID=1532

http://www.abntcatalogo.com.br/Norma.aspx?ID=306582

http://www.fieb.org.br/download/Senai/NBR_ISO_27002.pdf

http://www.security.usp.br/Palestras/Normas-Encontro-USP-Seguranca-Computacional-II-V-1-02.pdf

https://beytech.com.br/2015/10/21/Voce-sabe-a-importancia-de-um-firewall-para-a-sua-empresa

https://pt.wikipedia.org/wiki/Information_Technology_Infrastructure_Library

https://pt.wikipedia.org/wiki/ISO/IEC_17799

https://pt.wikipedia.org/wiki/ISO_27001

https://www.microsoft.com/pt-br/Security/resources/ransomware-whatis.aspx

http://www.fieb.org.br/download/senai/NBR_ISO_27002.pdf